Sample Security Procedures

Document number	PR-D2-0621
Revision	9.2
Date	December 2019
Synopsis	Sample security procedures to establish and maintain the security of a system using a Hardware Security Module (HSM), in particular the Prism TSM500i.

1. Introduction

High-security environments and devices operate on the principle of *managed security*: the environment or device must be managed according to established procedures in order to maintain the high level of security, and to detect and act against potential or real security threats.

This document is based on the requirements of:

- PCI PIN Security Requirements

This document is intended as a sample only:

- The procedures herein may be incomplete. Consult the latest PCI PIN Security Requirements to ensure compliance.
- The procedures should be customised for your particular environment.

2. Contents

1. INTRODUCTION **2**

2. CONTENTS **3**

3. KEY WORDS / PHRASES **5**

4. PERSONNEL PROCEDURES **7**

4.1 BACKGROUND CHECKS 7
4.2 PERSONNEL ROLES AND SECURITY PROCEDURES 7
4.3 SECURITY AWARENESS TRAINING 8
4.4 MANAGEMENT OF PERSONNEL CHANGES PROCEDURE 8

5. GENERAL SECURITY PROCEDURES **9**

5.1 PROCEDURE FOR VACATING THE CONTROLLED ENVIRONMENT 9

6. ACCESSING THE CONTROLLED ENVIRONMENT **10**

6.1 REQUIREMENTS 10
6.2 PROCEDURE FOR ACCESSING THE CONTROLLED ENVIRONMENT 10
6.3 ABORTING ACCESS TO THE CONTROLLED ENVIRONMENT 10

7. VACATING THE CONTROLLED ENVIRONMENT **11**

7.1 REQUIREMENTS 11
7.2 PROCEDURE FOR VACATING THE CONTROLLED ENVIRONMENT 11

8. PROCEDURE FOR PERIODIC SECURITY INSPECTION **12**

9. ASSIGNING CRYPTO OFFICERS **13**

9.1 HSM ACCESS CONTROL OVERVIEW 13
9.2 REQUIREMENTS 13
9.3 PROCEDURE TO ASSIGN A CRYPTO OFFICER 14
9.4 PROCEDURE TO REASSIGN OPERATOR ID TO A NEW CRYPTO OFFICER 14
9.5 PROCEDURE TO CHANGE CRYPTO OFFICER PASSWORD 14

10. PROCEDURE FOR COMMISSIONING A HSM **15**

11. PROCEDURE FOR KEY GENERATION **16**

11.1 REQUIREMENTS 16
11.2 PROCEDURE 16
11.3 ABORTING THE PROCEDURE 17

12. PROCEDURE FOR KEY COMPROMISE **19**

12.1 ROLES AND RESPONSIBILITIES 19
12.2 PROCEDURE 19

13. PROCEDURE FOR DESTRUCTION OF OBSOLETE KEYS **20**

14. PROCEDURES FOR STORING/RETRIEVING KEY COMPONENTS **21**

14.1 PROCEDURE FOR STORING KEY COMPONENTS 21
14.2 PROCEDURE FOR RETRIEVING KEY COMPONENTS 21

15. PROCEDURE FOR TRANSPORTING KEY COMPONENTS **22**

15.1 INSTRUCTIONS 22

16. PROCEDURE FOR KEY ENTRY/LOADING **23**

16.1 REQUIREMENTS 23
16.2 PROCEDURE 23
16.3 ABORTING THE PROCEDURE 24

17. INSTRUCTIONS FOR DATA BACKUP **25**

18. PROCEDURES TO MANAGE TSM-WEB USER ACCOUNTS **26**

18.1 REQUIREMENTS 26
18.2 INSTRUCTIONS 26
18.3 PROCEDURE TO ADD A USER ACCOUNT 26
18.4 PROCEDURE TO DISABLE A USER ACCOUNT 26

19. PROCEDURE FOR HSM DECOMMISSIONING 27

20. PROCEDURE FOR SYSTEM DECOMMISSIONING 28

21. ANNEX A: RECORD OF IDENTITIES OF SECURITY OFFICERS 29

22. ANNEX B: ACCESS CONTROL REGISTER 30

23. ANNEX C: INSPECTING CONTROLLED ENVIRONMENT EQUIPMENT 31

24. ANNEX D: COMPONENT SHEET 32

25. ANNEX E: COMPONENT ENVELOPE 33

26. ANNEX F: KEY REGISTER 34

27. ANNEX G: PASSWORD SHEET 35

28. ANNEX H: SECURITY AWARENESS TRAINING FORM 36

29. ANNEX I: PERSONNEL CHANGE FORM 37

3. Key Words / Phrases

The following key words indicate important concepts used throughout this procedural document. The key words or phrases have been italicised throughout the document.

Access Control Registry

This document is used to record all activity relating to the Controlled Environment. **Annex B** contains a sample page. This document must be accurately maintained at all times during the lifetime of the Controlled Environment.

Component

A component (as it is loosely referred to in this document) is a part of a cryptographic digital key, which, when combined with the other components using a logical XOR function, forms a complete cryptographic digital key. The major keys within the system are separated in this manner to ensure that no one person ever has access to all information needed to compromise the system.

Component sheet

This is the medium used to record components. When not in use they must be stored in a secure place such as a bank safety deposit box.

Custodian

A Custodian is a person charged with the responsibility of the safekeeping of a Component. This responsibility is of the highest degree of seriousness and failure to keep the Component secret is a serious offence.

Hardware Security Module (HSM)

Prism's TSM500i are Hardware Security Modules (HSM) which include a tamper responsive mechanisms certified to PCI HSM version 3 physical security.

Key Component Entry Device (KCED)

The KCED is a handheld device that connects over a serial interface to the dedicated CSP port on the TSM500i HSM. It is used by a Crypto Officer to enter their password when authenticating themselves to the HSM. The KCED is also used by each custodian when they enter their key component into the HSM.

Key Register

The Key Register is used to keep track of the details of any particular cryptographic key and the respective Custodians for that key. This information is essential for the identification and reconstruction of a particular key.

Labelled Envelope

This envelope is specially labelled according to **Annex D**. Completed Component Sheets and Password Sheets (if applicable) must be folded and stored in such envelopes before placement into their secure locations. The label on the envelope must be completed by the Custodian so as to record the identification of the Component for cross-referencing with the Key Register.

Crypto Officer Password

The HSM password is a 7-digit numerical value which, together with a Crypto Officer ID, is used to uniquely identify a Crypto Officer to an HSM. The requirement for the Crypto Officer passwords (2 will be required) to be entered when switching the HSM into a “Privileged Mode” allows for the strict enforcement of the procedural requirement for key loading to be supervised by Custodians.

Password Sheet

A sample password sheet is located in **Annex G** and must be used by Custodians to record their passwords for future reference. These password sheets must be stored in the Labelled Envelopes along with the Component Sheets when storing the Components.

Security Officer

The Security Officer is the person required to perform the procedures laid out in this document. Failure to perform this function exactly as specified in this document is a serious offence.

4. Personnel Procedures

The section describes the need for security awareness training, management of personnel changes.

4.1 Background checks

A background check should be done for all personnel involved in the system using the HSM. The motivation for this is that the personnel involved are required by the organisation operating the system to be trustworthy.

4.2 Personnel Roles and Security Procedures

The following table shows the security procedures and role players matrix:

Security Procedure	**Admin**	**Crypto Officer**	**Custodian**
Management of Personnel Changes Procedure	Yes		
Accessing the Controlled Environment	Yes	Yes	Yes
Vacating the Controlled Environment	Yes	Yes	Yes
Periodic Security Inspection		Yes	
Assigning Crypto Officers	Yes	Yes	
Procedure for HSM Commissioning	Yes	Yes	Yes
Procedure for HSM Decommissioning	Yes	Yes	
Procedure for System Decommissioning	Yes	Yes	
Procedure for Key Compromise	Yes	Yes	Yes
Procedure for Data Backup	Yes*		
Procedure for Key Generation	Yes	Yes	Yes
Procedure for Key Entry		Yes	Yes
Procedures for Storing/Retrieving Key Components			Yes
Procedure for Destruction of Obsolete Keys	Yes		Yes
Procedure for Transporting Key Components			Yes
Procedures to Manage Tsm-Web User Accounts	Yes		

* This procedure may be delegated to an IT support person

The Admin is the person who is the line manager who is responsible for the HSM and the procedures to manage it securely.

The Auditor role is not specifically shown in the table as the auditor reviews logs and forms that prove that the HSM is being managed in line with PCI PIN Security Requirements.

The above mentioned security procedures are covered in detail in this document. To execute a security procedure the relevant user manual may need to be referred to in addition to the Security Procedures in this document.

One person can have multiple roles as long as split knowledge of key components and dual control of the HSM is maintained. For example you could have a custodian who is a Crypto Officer or an Admin who is also a Crypto Officer.

4.3 Security Awareness Training

All personnel need to go through appropriate training for their responsibilities which includes the security procedures that apply to them. Once this training has been done they must fill in a form, see “Annex H: Security Awareness Training Form”, to provide proof.

4.4 Management of Personnel Changes Procedure

When there is a personnel change/move the “Annex I: Personnel Change Form” must be completed. This procedure is critical in nature and cannot be aborted.

5. General Security Procedures

General Security Procedures are rules instituted during the commissioning of the environment and the HSM and which must remain in effect until they are decommissioned. These procedures are intended to deter the theft or substitution of equipment or cryptographic keys by controlling physical access to the controlled environment in which the HSM is housed.

- General Security Procedures must be observed from the time of Commissioning until the Decommissioning is completed.
- The HSM must be housed in a controlled environment such that:
  - At least two trusted Security Officers are nominated and will be accountable for the security of the HSM and its environment. The identities and contact details of these individuals must be well known, and recorded at the entrance to the HSM environment. Annex A contains a sample form for recording the identities of the Security Officers.
  - Physical access to the controlled environment is restricted to trusted personnel (not necessarily the Security Officer).
  - A log of access to the controlled environment ("Access Control Register") is maintained and includes the following details: Name(s) of person(s) or equipment entering the environment, date and time or entry, purpose of entry. Annex B contains a sample *Access Control Register*.
  - No unauthorised persons may enter the controlled environment at any time. An authorised person is one who has legitimate business in the environment and has been granted access by a Security Officer.
  - There shall be no visual surveillance equipment within the controlled environment that is capable of zooming or focusing to a degree that would allow hand movements (such as key presses) to be identified.
  - No equipment or records may enter or leave the controlled environment unless such an event is logged on the Access Control Register *and* the event complies with a written procedure. These events specifically include backups for disaster recovery and HSM maintenance.
- Periodic security inspections must be performed on the controlled environment and the equipment it contains, to ensure compliance with the General Security Procedures. See the "Procedure for Periodic Security Inspection". Such inspections should occur at least once every 185 days.

5.1 Procedure for Vacating the Controlled Environment

Whenever the controlled environment is vacated (the last person who has been present is leaving) the equipment, software and environment must be correctly secured.

Procedure

- Close all access doors to the controlled environment and ensure that all locks on each door are locked.

6. Accessing the Controlled Environment

Whenever anyone enters the controlled environment the following procedure must always be followed.

6.1 Requirements

- The *Access Control Registry* must be present in the controlled environment at all times. If this document does not exist due to it being the first time that the controlled environment is used, the *Security Officers* are responsible to ensure that it gets created. The recommended *Access Control Registry* is in **Annex B**.

6.2 Procedure for Accessing the Controlled Environment

1. An *authorised person* must be present if the controlled environment is to be unlocked :

   The authorised person must sign the *Access Control Registry* indicating that they have unlocked the controlled environment.

2. Each authorised person must fill in the *Access Control Registry*, indicating the time of entering the controlled environment.
3. If the authorised person is accompanied by *an unauthorised person*, then they must record the reason that the person is entering the controlled environment in the *Access Control Registry*.
4. If the person is bringing any equipment whatsoever into the controlled environment then the details of the equipment must be entered into the *Access Control Registry* and must be signed by the person and by the *Security Officer* (if the person is not a *Security Officer*).

6.3 Aborting Access to the Controlled Environment

- This procedure may be aborted at any point before successfully completing the procedure. The *Security Officer* must cross out any entries into the *Access Control Registry* concerning the person aborting the entry. The *Security Officer* must also record that the person did not enter and initial it. If no entries were made, nothing else is required to abort the procedure.

7. Vacating the Controlled Environment

Whenever anyone leaves the controlled environment the following procedure must be followed.

7.1 Requirements

- The *Access Control Registry* must be present in the *Controlled Environment* at all times. This document must exist as the **Procedure for Accessing the Controlled Environment** specifies the creation of this document.

7.2 Procedure for Vacating the Controlled Environment

Note: This procedure may **not** be aborted.

1. The person must sign the *Access Control Registry*, indicating the time of exiting the controlled environment. The *Access Control Registry* must contain a record of the reason the person was in the *Controlled Environment*.
2. If the person above is an *unauthorised person*, the *authorised person* present must place their initials on the *Access Control Registry* next to the reason that the person was in the controlled environment. This is an indication that the *authorised person* is satisfied that the reason for the person being in the *Controlled Environment* is accurate and complete.
3. If the person is removing any equipment whatsoever from the controlled environment (all equipment must have been signed-in on entering the controlled environment) then the details of the equipment must be entered into the *Access Control Registry* and must be signed by the person and by the *Security Officer*.

In addition to the previous steps, the following steps must be executed by the last *authorised person* to leave the *Controlled Environment*:

4. The *authorised person* must ensure that the PC with the software application has been closed so that no unauthorised persons may operate it. This step must be executed in accordance with the manufacturers’ specifications for the respective systems.
5. Close all access door(s) to the controlled environment and ensure the door is locked.

8. Procedure for Periodic Security Inspection

Regular inspections of the controlled environment, its equipment and environment, and the adherence to procedures are required to maintain the security of the environment.

Instructions

- This procedure must be executed by a Security Officer, and may not be delegated to any other person.
- The procedure must be executed at least once every 185 days.

Procedure

- Inspect the controlled environment
    - *Access Control Register* exists at the entrance to the controlled environment and is up to date. Identities of Security Officers are recorded in plain view.
- Inspect the equipment
    - Inspect all HSMs for signs of physical tampering, as described in Annex C. Use appropriate software to check that no HSMs are in a tamper state.
    - Inspect all other equipment for unauthorised modification (an inspection checklist should be created for this purpose).
- Procedure check
    - The *Access Control Register* is present and up to date.
    - The *Key Register* is present.
    - A copy of this procedure document is present and readily available within the controlled environment.

9. Assigning Crypto Officers

9.1 HSM Access Control Overview

Access control to the HSM is managed via an identity-based authentication system. PCI PIN Security requirements requires the HSM to be managed under dual control. Dual control is achieved by requiring two crypto officers to authenticate themselves to the HSM application before it will permit certain security sensitive operations to be done, such as:

- Key component entry via the Key Component Entry Device (KCED)
- Enable terminal key injection for a session

The purpose of dual control is to prevent any one operator of HSM from performing security sensitive tasks alone.

The crypto officer can also do the following when the HSM Boot Loader is running:

- Set tamper
- Clear tamper
- Set date and time
- Change own password

There are 2 predefined crypto officers (Operator ID = 1 and Operator ID = 2). The password is alphanumeric and upon correct authentication, the role is selected based on the operator ID of the crypto officer.

Operator IDs 1 and 2 are to be assigned to particular operators (crypto officers) and are not to be treated as general-purpose role-based logins.

The TSM500i HSM allows for additional crypto officers by creating additional Operator IDs. If this is required for operational reasons, e.g. one of the primary crypto officers is on leave or away on business, then these can be created by asking the manufacturer for a digital signature for each additional Operator ID.

9.2 Requirements

The operator IDs must be managed strictly in accordance with the following rules:

- There must be a pen-and-paper procedure that assigns a unique individual to one of the predefined crypto officer Operator IDs.
- No individual may be assigned to more than one operator ID, and no operator ID to more than one individual
- Each individual is responsible for setting their password themselves, and thereafter ensuring the secrecy of the password. In particular it must never be disclosed to anyone else (not even another officer or user), must not be written down, and must not be stored on an electronic medium. However, the following are acceptable:
    - It may be stored in a safe and the key/combination to the safe must be under the sole control of the individual.
    - Stored encrypted on an electronic medium where a strong encryption algorithm is used and the information necessary to decrypt the password is itself treated according to these rules. In other words, if an action is taken using a particular operator ID, there is one and only one person that could have performed that action, and will be presumed to be responsible.
- Failure to follow these rules will result in disciplinary action as it could compromise the security of the HSM and the system in which it is used.

Operator ID 3 is a predefined crypto user. This operator is not able to perform any security relevant functions and as such the default password can be left unchanged.

9.3 Procedure to assign a Crypto Officer

- Identify suitable trusted individual
- Take the person through the responsibilities of crypto officers stressing the
    - Need to keep their password secret
    - Importance of dual control
    - Failure to comply will result in disciplinary action
- Provide security awareness training
- Record the crypto officer identity on the **Record of Identities of Security Officers** form
- The **Record of Identities of Security Officers** form must be filed for future reference.

9.4 Procedure to reassign Operator ID to a new Crypto Officer

- Outgoing Crypto Officer to logon for the specific Operator ID affected. If this is not possible they should give their password to the new Crypto Officer with another Officer as witness.
- The new Crypto Officer must change the password for the specific Operator ID affected immediately. See “Procedure to change Crypto Officer password”
- Record that the person previously assigned to the specific Operator ID is no longer assigned by updating the relevant Record of Identities of Security Officers form
- Follow the “Procedure to assign a Crypto Officer” above for the new Crypto Officer.

9.5 Procedure to change Crypto Officer password

- Log on to the HSM with assigned Operator ID using the existing Crypto Officer password
- Record new password on the “Annex G: Crypto Officer Password Sheet” form
- Change the Crypto Officer password
- Securely store the Crypto Officer Password Sheet form.

10. Procedure for Commissioning a HSM

Each HSM must be commissioned prior to use. The process ensures that the HSM is authentic, that its access control mechanisms are correctly configured, and that it securely stores the correct SMK necessary for operation in the system.

Requirements

- At least two Security Officers
- All SMK custodians (with their SMK components)
- One or more HSMs to be commissioned

Procedure

- The HSM must be inspected according to the manufacturer's guidelines to ensure its authenticity and that it does not show signs of tampering. See Annex C for further details. The manufacturer must warrant that the HSM conforms to the definition[1] of a Tamper Responsive Security Module that relies only on physical barriers.
- Initialise the HSM with Access Control users and passwords according to "Procedure to establish Access Control".
- If the SMK components have not yet been generated[2], they should be generated now according to the "Procedure for Key Generation".
- The SMK must be loaded by following the "Procedure for SMK Loading".
- HSM commissioning is complete.

[1] According to ANSI, ISO, VISA and MasterCard's specifications

[2] It should only be necessary to generate SMK components when the first HSM of the system is being commissioned.

11. Procedure for Key Generation

This is the procedure for generating a key in component form using the *Prism* TSM500i HSM. The procedure also addresses the recording of the key components by the custodians.

The HSM controls the KCED. Each component is shown in turn on the KCED screen. The process can be aborted by pressing the cancel key on the KCED which causes the HSM to stop showing the key components via the KCED screen.

11.1 Requirements

- Two *Security Officers* must be present.
- All Key *Custodians*
- This procedure must be done under the principles of split knowledge and dual control so that ant one person is prevented from having access to all the components.
- A *Key Register* (the recommended Key register is available in **Annex E**) - If one does not exist.
- Stationery for recording and securely storing the key *components*, in particular:
  - Pens with indelible ink for *Custodian*s
  - *Component Sheets* (we recommend two per *Custodian* – the recommended key component sheet is available in **Annex C**). The benefit of two component sheets is that the one sheet will serve as a backup record which can be stored securely off site. The use of carbonised sheets obviates the necessity of having to fill in the key details twice.
  - *Labelled Envelopes* (at least two per *Custodian* – the recommended envelope label is available in **Annex D**). Once the envelopes are sealed we recommend that tamper-evident stickers be placed over the seal.
- Upon completion of the key generation, each *Custodian* must have access to a lock-up safe and if they created a backup then a second safe in a different, physical building.
- Key generation must be performed in a controlled environment.
- The task of the *Security Officer* is to implement and enforce the following procedures and thereby guide the *Custodian*s through the process of generating their respective *components*.
- Unencrypted key *components* must, at all times, only be in the custody of the respective *Custodian*s, or in a secure tamper-evident container.

11.2 Procedure

The following procedure must be followed in the sequence specified.

1. The *Security Officer(s)* must inspect the HSM and KCED, according to the manufacturer’s guidelines, to ensure its authenticity and that it does not show signs of tampering.
2. The cable used to connect the KCED to the HSM must be inspected by the *Security Officer(s)* to ensure that there are no unauthorised modifications to the cables.
3. The KCED must be connected to the HSM as described in the KCED Installation and User Guide.
4. The *Custodians* shall establish the name for the key. For example “HSM Storage Master Key – Live”.
5. The identity of all *Custodian*s and the key name shall be recorded in the “Key Register”.

6. The *Security Officer* shall provide each *Custodian* with two *Labelled Envelopes* and "Component Sheets".
7. The *Custodian*s shall title the *Labelled Envelopes* and "Component Sheets" with the agreed name, and the identities of all *Custodian*s must be recorded on each envelope. If used, the second "Labelled Envelope" and "Component Sheet" for each *Custodian* should additionally be subtitled "Backup".
8. Crosscheck steps 4 – 7 above to ensure that all key *Custodian*s have accurately recorded the key name and the *Custodian* identities.
9. From this point on, **no one** is permitted to view another *Custodian's Component Sheet*. Each key *component* is **secret**, and must not be revealed to anyone else. Each *Custodian* must take the utmost care to preserve the secrecy of his or her component during and after the key generation procedure.
10. The *Security Officer(s)* must operate the HSM at this point and place it in the key component generation mode. The *Security Officer* must provide all information that the HSM requires, but must stop when the KCED requests that the first *Custodian* assume control of the KCED.
11. The First *Custodian* must assume control of the KCED at this point. Everyone else is required to exit the *Controlled Environment*. The door must be closed and everyone is required to wait outside until the *Custodian* has completed the generation of his or her *component*.
12. The *Custodian* must follow the on-screen instructions of the KCED until a key component is displayed.
13. The *Custodian* must then record the component onto their *Component Sheet(s)*. The *component* will be presented as groups of sixteen hexadecimal digits. The custodian must ensure than this is done in such a way that no one else is able to view the component or the component sheet.
14. Only once the <u>component</u> is recorded on **all** *Component Sheets* may the *Custodian* proceed with the on-screen instructions on the KCED. The *Custodian* must then proceed until the **component** *check value* is displayed, and then record the **component** check value onto **all** of their *Component Sheets*. The *check value* will be presented as six numerical digits.
15. Only once the <u>component check value</u> is recorded on **all** "Component Sheets" may the *Custodian* proceed with the on-screen instructions on the KCED. The *Custodian* must then proceed until the key *check value* is displayed, and then record the *check value* onto their *Component Sheet(s)*. The *check value* will be presented as six numerical digits.
16. Only once the <u>*key check value*</u> is recorded on **both** "Component Sheets" may the *Custodian* proceed with the on-screen instructions on the KCED. The *Custodian* must then proceed until the KCED requests that it be handed over to the next key *Custodian*.
17. Steps 11-16 above must be repeated for *Custodian*s 2 and 3 (if a third *Custodian* is used) respectively. Please note that the last *Custodian* will not be prompted to pass the KCED to the next *Custodian*, but will instead be informed that the key *component* generation has been successful.
18. If the key components are to be entered into the HSM immediately after being generated then the custodians do not need to seal their envelopes immediately. Otherwise the components should be sealed in their envelopes and stored as per the Procedure for Storing Key Components.

11.3 Aborting the Procedure

The following steps must be taken to abort the key Generation Procedure.

1. The reason for aborting of the generation must be recorded on the *Key Register*.
2. If generation of the key specified in the *Key Register* is <u>not to be</u> reattempted, the *Key Register* must be filed for future reference.

3. The *Security Officer* must press the cancel key on the KCED in order to abort the generation/confirmation of key *components* (if the KCED has not already exited these processes).

4. All *Component Sheets* must be destroyed as per the "Procedure for Destruction of Obsolete Keys". *Labelled Envelopes* need only be destroyed if the previously generated key-check value has already been recorded on them, or if key generation is not to be reattempted.

5. If key generation is to be reattempted, record on the *Key Register*, that regeneration of the key is commencing. The reattempt must commence immediately.

6. If key generation is not to be reattempted, then the *Controlled Environment* should be vacated (see the procedure "Vacating the Controlled Environment").

12. Procedure for Key Compromise

This procedure describes the process to be followed in the event of a key, or any of the key components of a key, used on the system being compromised.

This procedure constitutes a response plan for a key compromise incident in order to react effectively and in a timely manner.

12.1 Roles and Responsibilities

- The security-sensitive keys that are capable of being compromised are keys that are entered into the HSM as components.
- The compromise of the Storage Master Key (SMK) will entail a re-keying of the system as all keys used by the HSM should be considered compromised.
- The resolution to the key compromise shall be a joint effort between the Custodians of the affected key(s).

12.2 Procedure

- Key owner(s) shall determine that a key compromise has occurred.
- The security breach shall be escalated to management of the organisation(s) owning the key(s).
- The use of the key(s) in the HSM shall be halted.
- The HSM shall be re-keyed:
    - All records of existing compromised keys shall be destroyed. Refer to the “Procedure for the Destruction of Obsolete Keys”.
    - The generation, injection and management of new keys shall be performed in accordance with this document.
- The key(s) in all affected devices sharing affected keys with the HSM will also need to be re-keyed.

13. Procedure for Destruction of Obsolete Keys

ISO 9564-1 2002 Appendix F.6 states that for paper materials (which in this context are component sheets and envelopes) are to be "destroyed by burning, pulverizing or cross-cut shredding. When material is pulverized, all residue is reduced to pieces 5 mm or smaller. When material is burned, the residue is reduced to white ash".

14. Procedures for Storing/Retrieving Key Components

This procedure covers the storage of paper key components and when key components need to be retrieved from storage. This would typically be for key entry, re-assignment of the component (due to personnel changes) or the destruction of an obsolete key.

14.1 Procedure for Storing Key Components

This procedure is critical in nature and may not be aborted. The Custodians must complete all of the following steps:

- The Key Component Sheets (and Password Sheets if they are available) must be sealed in the Labelled Envelopes for transport and storage. Once the envelopes are sealed we recommend that tamper-evident stickers be placed over the seal.
- Verify that all envelopes are sealed as stated above.
- The Custodians must immediately go to the lock-up safes reserved for their components. NB. There must be a separate physical location (in a different building) assigned for each component and the component's backup, should backup components be used.
- Only the appointed primary (and backup if appointed) Custodian should have access to the specific key component required

14.2 Procedure for Retrieving Key Components

This procedure is critical in nature and may not be aborted. The Custodians must complete all of the following steps:

- Access to key components must be limited to a need to know basis so that the fewest number of key custodians are necessary to enable their effective use.
- Only the appointed primary (and backup if appointed) custodian should have access to the specific key component required
- Check that the Key Component Sheets (and Password Sheets if they are available) are sealed in the Labelled Envelopes for transport and storage.
- Check that all envelopes are sealed as stated above.
- All Custodians and Security Officers must sign the Access Control Registry noting the purpose for which the key components were removed from storage. This is necessary for audit trail purposes as all use of the key components needs to be recorded.
- Each Custodian shall then use their component as noted in the Access Control Registry.
- Each Custodian must store their component as described in "Procedure for Storing Key Components"

15. Procedure for Transporting Key Components

This is the procedure covers the manual transportation of paper based key components. This would typically be followed once the component has been removed from its place of storage to a location where it needs to be loaded into another HSM. This procedure is followed when a key shared between two HSMs for example a Key Encryption Key (also referred to as a Zone Master Key).

15.1 Instructions

- The purpose of this procedure is to ensure that the split knowledge is preserved.
- The component needs to be under the continuous supervision of the key custodian who is authorised to access this component.
- The component sheet must only be visible to the authorised key custodian long enough for them to enter it privately into a HSM.
- If any of the key custodians fails to follow these instructions then the key component will be deemed to be compromised.

16. Procedure for Key Entry/Loading

This is the procedure for entering a key in component form using the *Prism* KCED (Key Component Entry Device).

16.1 Requirements

- Both *Security Officers* must be present for the whole procedure.
- All key *Custodian*s (with their key *components* at hand – please see "Procedure for Retrieving Key Components" for details on obtaining these *components*)
- This HSM must have been inspected to ensure authenticity and that it does not show signs of tampering.
- This procedure must be done under the principles of split knowledge and dual control so that ant one person is prevented from having access to all the components.
- The KCED Installation and User Guide
- The Tsm-Web User Guide
- *Key Register* – this document should have been generated during key generation.
- *Access Control Registry* – must be present.
- *KCED* – Key Component Entry Device

16.2 Procedure

1. The cable used to connect the KCED to the HSM must be inspected by the *Security Officers* to ensure that there are no unauthorised modifications to the cables.
2. The KCED must be connected to the HSM as described in the KCED Installation and User Guide.
3. Each *Security Officer* shall login to the HSM by entering there password. Once this has been completed the HSM will enter the privileged state which allows key components to be loaded.
4. Once the HSM is in the privileged state the software driving the HSM will request the HSM to load a particular type of key e.g. Storage Master Key, Key Encryption Key etc. Follow these instructions until the KCED requests that the first key *Custodian* assume control of the KCED.
5. All other people must be sufficiently far away to allow the active *Custodian* to securely enter their component i.e. it must not be possible for the other people present to observe the component sheet.
6. The *Custodian* will be prompted to enter their component; verify their component check value.
7. After successfully completing steps 5-6 above, the active *Custodian* will be prompted to pass control of the KCED to the next *Custodian*. Steps 7-8 must be repeated until all *Custodian*s have entered their *components*.
8. The *Security Officer* must verify that the KCED indicates that the key has been successfully loaded. The key check value must be verified.
9. Record the details of the HSM (including its serial number) on the "Key Register".
10. If additional keys need to be loaded then repeat steps 5-9 until all keys have been loaded.
11. The *Security Officer* must verify that the HSM is returned to the operational state after key loading is complete. This is to prevent unauthorised key entry.

16.3 Aborting the Procedure

This procedure may be aborted by anyone at any time. Reasons for aborting might include but are not limited to the following:

- Equipment has been tampered with.
- Part or all of a component has been compromised.
- Collusion between key *Custodian*s is suspected.
- Initialisation of the HSM is no longer deemed to be necessary.

Please note that abortion of this procedure (except in the case of the fourth point above) implies either a serious error, or a breach of security. Full details in both the “Key Register” and the *Access Control Registry* are to be provided.

An immediate resolution for the problem must be arranged. It is not within the scope of this document to discuss this resolution with the exception of the following: In the event of a security breach, the resolution must include the destruction of the current key. In this event a new key must be generated.

17. Instructions for Data Backup

Data in the controlled environment must be regularly backed-up to ensure system recovery in the event of a failure. Procedures must be in place to identify the data components to be backed up.

Instructions

- Identify and authorise a trusted individual to be responsible for managing backups of the system.
- Identify a secure off-site facility (geographically remote) for the storage of the backups.
- Identify a trusted individual or courier company to transport the backups to the off-site facility.
- Backup the data regularly to removable medium and ensure that the backup is recoverable and generally error-free.
- Remove the backup medium from the controlled environment and log both the backup and the removal on the Access Control Register.

18. Procedures to Manage Tsm-Web User Accounts

The Tsm-Web allows for users to have an Admin role or an Operator role. A more detailed description of these roles is provided in the Tsm-Web User Manual.

18.1 Requirements

- Audit guidelines require that each user of the Tsm-Web must be uniquely identified.
- Users may not share their password with any other user or un-authorised individual.
- A user who is no longer authorised to use the Tsm-Web should have their account disabled or removed.

18.2 Instructions

- It is the responsibility of the organisation operating the Tsm-Web to ensure that the above requirements are met following the procedures below.

18.3 Procedure to Add a User Account

1. The Tsm-Web User Setup section of the Tsm-Web User Manual provides the details on how to add user accounts.
2. A user with a Security Officer role needs to log into the Tsm-Web application as this role is required for user management.
3. Make sure that the new user is assigned a unique username and set their role according to their responsibility. Create the user account and have the user enter their password.

18.4 Procedure to Disable a User Account

1. The Tsm-Web User Setup section of the Tsm-Web User Manual provides details on how to disable user accounts.
2. A user with an Admin role needs to logon to the Tsm-Web application as this role is required for user management.
3. Select the applicable user account and set their role to none or expire the user account.

19. Procedure for HSM Decommissioning

The HSM stores security-sensitive information that must be irrecoverably destroyed when the HSM is no longer required.

Instructions

- The decommissioning of the HSM must be performed under dual control.
- Security-sensitive data must be removed from the HSM when it is taken out of service.
- The HSM manufacturer's guidelines shall be followed to cause a hardware destruct event that is guaranteed to irrecoverably destroy the security sensitive information in the HSM.
- Any HSM access control passwords that have been written down must be brought into the controlled environment, prove they are sealed and then destroyed.
- The HSM must be removed from the controlled environment and the decommissioning and removal must be logged on the Access Control Register.

20. Procedure for System decommissioning

This procedure described the guidelines to decommission the system in the controlled environment when the system is no longer required.

Instructions:

- The system decommissioning must be performed by two people to ensure accountability.
- Decommission all HSMs. See section “Procedure for HSM Decommissioning”.
- Destroy all key databases outside the HSM(s).
- All security-sensitive information must be brought in by their custodians, prove that they are sealed and then destroyed. This includes key custodians and their key component envelopes.
- Remove all system equipment from the controlled environment and log it out on the Access Control register.
- Retrieve and destroy all off-site backups.
- Retain all procedural records (Access Control Register, Key Register, etc) for a minimum of 5 years.

21. Annex A: Record of identities of Security Officers

Complete this sheet and place a copy of it at the entrance to the controlled environment. Make additional copies of this page as required.

CONTROLLED ENVIRONMENT

NO UNAUTHORISED PERSONS ARE PERMITTED BEYOND THIS POINT

RULES

- ALL PERSONS AND EQUIPMENT ENTERING OR LEAVING THIS SECURE ENVIRONMENT MUST BE LOGGED ON THE ACCESS CONTROL REGISTER.
- ALL AUTHORISED PERSONS ARE TO BE SUPERVISED BY A SECURITY OFFICER.
- ACCESS TO THIS CONTROLLED ENVIRONMENT IS UNDER DUAL CONTROL. TWO SECURITY OFFICERS ARE REQUIRED TO UNLOCK THIS DOOR.
- A SECURITY OFFICER MUST INSPECT AND SECURE THE ENVIRONMENT WHEN THE LAST PERSON LEAVES.

A FULL COPY OF THE PROCEDURES MANUAL FOR THIS CONTROLLED ENVIRONMENT (DOCUMENT PR-D2-0621 REVISION 9.1) IS AVAILABLE FROM:

NAME AND CONTACT DETAILS OF PERSON WHO CAN PROVIDE THE DOCUMENT

SECURITY OFFICERS

SECURITY OFFICER # 1

FULL NAME AND CONTACT DETAILS

SECURITY OFFICER # 2

FULL NAME AND CONTACT DETAILS

SECURITY OFFICER # 3

FULL NAME AND CONTACT DETAILS

TRUSTED PERSONS *WHO MAY BE IN THIS CONTROLLED ENVIRONMENT UNSUPERVISED*

FULL NAME AND CONTACT DETAILS

AUTHORISED BY (OFFICER NAME & SIGNATURE)

FULL NAME AND CONTACT DETAILS

AUTHORISED BY (OFFICER NAME & SIGNATURE)

FULL NAME AND CONTACT DETAILS

AUTHORISED BY (OFFICER NAME & SIGNATURE)

22. Annex B: Access Control Register

Use this sheet to create and maintain an Access Control Register. The register should be placed at the entrance to the secure environment, and can be conveniently kept as a file or loose-leaf records. Makes copies of this page as required.

Page # Number pages in order starting at "1"

- Log equipment in and out in separate entries where that equipment will stay in the Controlled Environment for a period of time.

Date & Time	Names of persons *or* equipment and direction (IN/OUT)	Purpose	Signatures of all persons (incl. Security Officers)
IN: OUT:			
IN: OUT:			
IN: OUT:			
IN: OUT:			
IN: OUT:			
IN: OUT:			
IN: OUT:			

23. Annex C: Inspecting controlled environment equipment

For the inspection, instructions provided by the manufacturer (or a representative) of the respective equipment shall be followed.

The following equipment within the controlled environment needs to be inspected:

- Server(s) and software.
- All Hardware Security Modules (HSMs) used in the controlled environment.
- All cables used to connect the system to HSMs or to other equipment (such as a KCED).

For each piece of equipment (hardware or software) there needs to be a guide to inspect the equipment to ensure that it is authentic and shows no evidence of tampering.

24. Annex D: Component Sheet

<u>CONFIDENTIAL</u>

DO NOT ALLOW ANY UNAUTHORISED PERSONS (INCLUDING OTHER CUSTODIANS OR SECURITY OFFICERS) TO SEE THIS COMPONENT.

Respect the following rules of key component security

- Each key component is **secret**, and must not be revealed to anyone. It must **never** be possible for a custodian to possess more than one component of a key.
- When not in use this component must be kept in a sealed, tamper-evident package and stored in a secure, tamper-evident container such that only the person with authorised access to the component can obtain it. In other words: seal this page in an opaque envelope and lock it in a safe to which only you have the key.

Key name ______________________________

Identifying name or description of the key

Institution ______________________________

Name of the institution that "owns" this component

Date ______________________________

YYYY/MM/DD of key / component creation

Generated by ______________________________

Full name and contact number of custodian (at key generation)

Component number ______ *of* _______ <u>Algorithm (circle one right):</u> AES / TDES

Component *Fill in those parts that are applicable.*

Part 1: *(For 128, 192 & 256 bit AES keys / single, double & triple length DES keys)*

□□□□ □□□□ □□□□ □□□□

Part 2: *(Only for 128, 192 & 256 bit AES keys / double & triple length DES keys)*

□□□□ □□□□ □□□□ □□□□

Part 3: *(Only for 192 & 256 bit AES keys / triple length DES keys)*

□□□□ □□□□ □□□□ □□□□

Part 4: *(Only for 256 bit AES keys)*

□□□□ □□□□ □□□□ □□□□

Component Check value

□□□□□□

<u>Key Check Value Algorithm (circle one below):</u>

Key Check Value

□□□□□□

Encrypt zeros (Legacy) / SHA256 / CMAC-based

25. Annex E: Component envelope

Use this sheet as a sample for the creation of uniquely numbered envelopes for protecting key components.

CONFIDENTIAL – CONTAINS KEY COMPONENT

Key name ______________________________

Key check value ____________ Component ___ of ___ Algorithm: AES / TDES

Institution (owner) ______________________________

Custodians CUSTODIAN # 1 ______________________________

(with contact numbers) CUSTODIAN # 2 ______________________________

CUSTODIAN # 3 ______________________________

Date sealed ______________

26. Annex F: Key Register

Use this sheet to create and maintain a Key Register that will record access to Critical Security Parameters (such as the SMK). Make copies of this page as required. The Key Register can be conveniently kept as a file of loose-leaf records.

Record # Number records in order starting at “1”

Date

YYYY/MM/DD of key access

Key name

Name or description of key accessed

Key check value

Print in block letters / digits

Key Algorithm (circle one) TDES / AES

Key check value Algorithm (circle one) TDES / CMAC / SHA256

Nature of access

Key generation or Key loading

Auditor(s)

[optional]

Full name(s) and contact number(s) of auditors present

Custodian #1

Full name and contact number of Custodian #1

Unique numbers of envelopes opened or sealed (indicate which)

Custodian #2

Full name and contact number of Custodian #2

Unique numbers of envelopes opened or sealed (indicate which)

Custodian #3

Full name and contact number of Custodian #3

Unique numbers of envelopes opened or sealed (indicate which)

Signatures

Signatures of all custodians, an auditor and a Security Officer

ANY ALTERATIONS ON THIS PAGE MUST BE SIGNED

27. Annex G: Password Sheet

Use this sheet to record passwords that are used to authenticate Administrators to Tamper Responsive Security Modules. Make copies of this page as required.

CONFIDENTIAL

DO NOT ALLOW ANY UNAUTHORISED PERSONS (INCLUDING OTHER CUSTODIANS OR SECURITY OFFICERS) TO SEE THESE PASSWORDS.

Password # NUMBER PASSWORDS IN ORDER STARTING AT "1"

Date ____________________
YYYY/MM/DD OF PASSWORD CREATION

Custodian ____________________
FULL NAME AND CONTACT NUMBER OF PASSWORD CREATOR

HSM Identification ____________________
SERIAL NUMBER OR OTHER IDENTIFICATION

Password ____________________
PRINT IN BLOCK LETTERS / DIGITS

Password # NUMBER PASSWORDS IN ORDER

Date ____________________
YYYY/MM/DD OF PASSWORD CREATION

Custodian ____________________
FULL NAME AND CONTACT NUMBER OF PASSWORD CREATOR

HSM Identification ____________________
SERIAL NUMBER OR OTHER IDENTIFICATION

Password ____________________
PRINT IN BLOCK LETTERS / DIGITS

Password # NUMBER PASSWORDS IN ORDER

Date ____________________
YYYY/MM/DD OF PASSWORD CREATION

Custodian ____________________
FULL NAME AND CONTACT NUMBER OF PASSWORD CREATOR

HSM Identification ____________________
SERIAL NUMBER OR OTHER IDENTIFICATION

Password ____________________
PRINT IN BLOCK LETTERS / DIGITS

28. Annex H: Security Awareness Training Form

This form must be filled in by the person who has been given security awareness training.

I have received training in the following areas (please tick or mark n/a)	**YES**	**NO**
Management of Personnel Changes Procedure		
Accessing the Controlled Environment		
Vacating the Controlled Environment		
Periodic Security Inspection		
Assigning Crypto Officers		
Procedure for HSM Commissioning		
Procedure for HSM Decommissioning		
Procedure for System Decommissioning		
Procedure for Key Compromise		
Procedure for Data Backup		
Procedure for Key Generation		
Procedure for Key Entry		
Procedures for Storing/Retrieving Key Components		
Procedure for Destruction of Obsolete Keys		
Procedure for Transporting Key Components		

I am aware that failure on my part to follow procedures may compromise the security of system and this will result in disciplinary action.

Date: ____________________

Name (in full): ____________________ **Signature:** ____________________

29. Annex I: Personnel Change Form

This form must be filled in by a security offer when there is a personnel move/change. All access control and other privileges must be revoked.

Please tick or mark n/a	**YES**	**NO**
Revoke access control to the operational facility		
Revoke user access to the Tsm-Web		
Change HSM Crypto Officer password		
Hand over key component(s) to the custodian who will replace this person		

I am aware that failure on my part to follow procedures may compromise the security of the system and this will result in disciplinary action.

Date: ____________________

Name (in full): ____________________ **Signature:** ____________________

Security Officer (print name): ____________________ **Signature:** ____________________